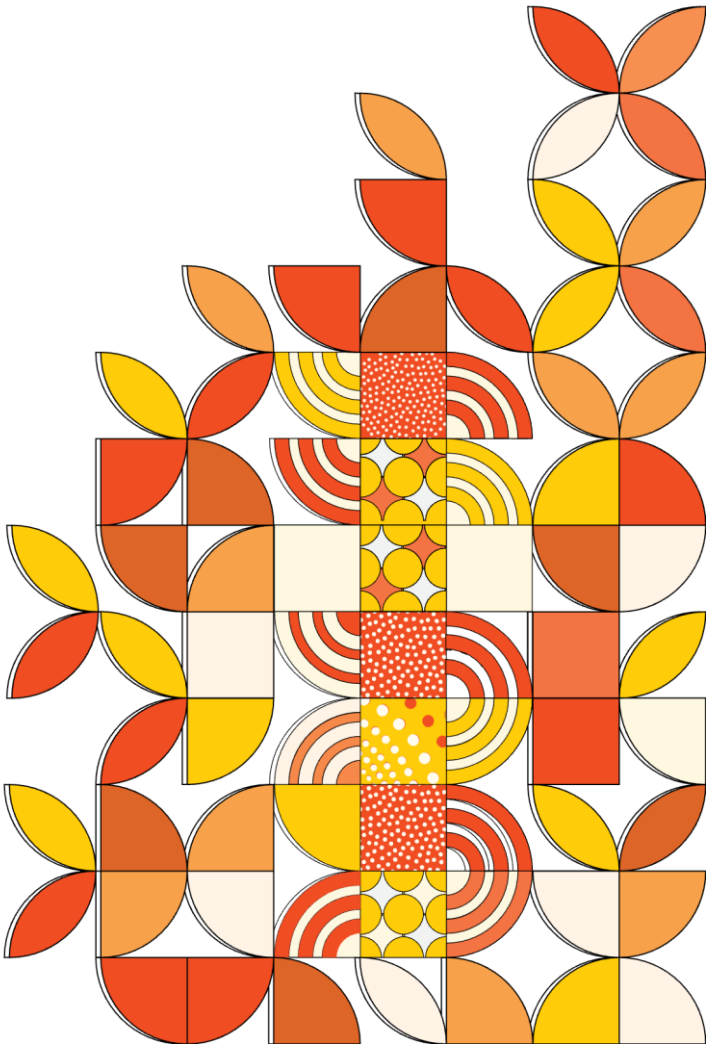
Legal entity: INSTITUTE OF HEALTH & MANAGEMENT PTY LTD.
Category: Institute of Higher Education
CRICOS Provider: 03407G| Provider ID: PRV14040
ABN: 19 155 760 437 | ACN: 155 760 437

Cyber Safety and Security Policy



www.ihm.edu.au
enquiry@ihm.edu.au

EDUCATION for EMPLOYMENT:
Bridging the gap globally

SECTION 1

Purpose

1. The purpose of this policy is to establish comprehensive guidelines for the responsible and secure utilisation of information and communication technologies at the Institute of Health & Management (IHM).
2. This document delineates precautionary measures and protocols to mitigate potential risks associated with the use of such technology within the organisation.

Scope

3. This policy applies to all staff, students, and stakeholders, including members of various governance committees at IHM.

Definitions

4. Definitions for key terms are presented in the Glossary of Terms.

Suite documents

5. This Policy is linked to the following:
   a) Cyber Safety and Security Procedure
   b) See also Associated Information listed in the 'Related Internal Documents' in Section 4 below.

SECTION 2

Policy Guidelines

6. **Cyber Security Threats**
   6.1 Cybersecurity is crucial for maintaining the confidentiality, integrity, and availability of information by defending against both malicious and accidental threats.
   6.2 These threats exploit vulnerabilities in technology, human actions, and processes to compromise information.
   6.3 To address these challenges, IHM constantly updates and implements cybersecurity mitigation strategies that are aligned with Victoria's Cyber Strategy and other relevant standards.

7. **Incident Response Plan**
   7.1 IHM will maintain a detailed incident response plan outlining specific steps to be taken in case of a data breach or cybersecurity incident.

7.2 This plan will ensure quick and efficient responses, minimising potential damage and ensuring compliance with legal requirements.

8. **Regular Training and Awareness Programs**

8.1 IHM will implement mandatory, regular cybersecurity training and awareness programs for staff, students, and stakeholders.

8.2 This ensures everyone is updated on the latest threats and best practices, reducing human error and enhancing overall security.

9. **Periodic Audits and Assessments**

9.1 IHM will conduct regular security audits and risk assessments to identify and mitigate vulnerabilities, ensuring continuous improvement and compliance with the latest cybersecurity standards and regulations.

10. **Data Encryption**

10.1 All sensitive data, both at rest and in transit, must be encrypted. This protects sensitive information from unauthorised access, even if data is intercepted or accessed inappropriately.

11. **Access Controls and User Permissions**

11.1 IHM will implement stringent access controls, ensuring users only have access to the data necessary for their role and minimising the risk of data breaches by limiting access to sensitive information.

12. **Multi-Layered Security Approach**

12.1 IHM will adopt a multi-layered security approach, including firewalls, intrusion detection systems, and endpoint protection, to provide comprehensive protection against various types of cyber threats.

13. **Backup and Recovery Procedures**

13.1 IHM will enhance backup and recovery procedures to ensure quick restoration of data and services in case of a cybersecurity incident, minimising downtime and data loss.

14. **Monitoring and Reporting Mechanisms**

14.1 IHM will develop robust monitoring and reporting mechanisms to detect and respond to suspicious activities promptly, enhancing the ability to identify and address potential security incidents in real time.

15. **Compliance with Updated Regulations**

15.1 IHM will regularly review and update the policy to ensure compliance with the latest local, national, and international regulations, maintaining legal compliance and demonstrating a commitment to upholding high-security standards.

16. **Passwords**

16.1 All stakeholders at IHM are expected to implement Multi-Factor Authentication (MFA) for their system and application logins.

16.2 Where applicable, IHM will ensure login through Single Sign-On (SSO) features, requiring MFA for those users.

16.3 Users will be required to use strong passwords, including a combination of uppercase, lowercase, numbers, and special characters, based on Microsoft Password Policy Recommendations and other regulatory guidelines.

17. **Use of Social Media**

17.1 Social media plays a significant role in educational settings, offering a valuable platform for engagement.

17.2 IHM staff, stakeholders, and students are permitted to engage in online communication platforms but must seek approval from the IHM Quality Assurance department to use the IHM logo or trademark. The logo must be used within style guides specified by IHM and must not be altered or defaced.

18. **Email Security Measures**

18.1 IHM staff and students are advised not to use their official email ID to register on unsolicited websites.

19. **Handling Materials Under Copyright**

19.1 IHM adheres to a Copyright Policy and Procedure and complies with applicable laws regarding copyrighted data.

19.2 The Unauthorised distribution or publication of copyrighted materials without the copyright holder's permission is prohibited.

20. **Cyber Bullying**

20.1 IHM prohibits any form of intimidation, threats, belittling, degradation, or bullying among community members.

20.2 Students should report incidents to student support or academic staff, while staff should report to IT support.

20.3 Victims of cyberbullying will be provided with assistance such as counselling and advice.

21. **Computer Viruses and Malware**

21.1 Security measures, including firewalls and anti-virus software, are in place for all IHM staff computers.

21.2 Students should install anti-virus software on personal computers used for IHM studies and report any detected viruses or malware to IT Support for appropriate action.

22. **Disclosure of Private Information**

22.1 Unauthorised disclosure of private information is a serious offence.

22.2 Affected individuals will be notified promptly.

22.3 , Staff or students found breaching privacy or confidentiality will face formal reporting and appropriate action.

22.4 Financial institutions must be informed immediately in cases involving financial details.

23. **Loss of Data**

23.1 IHM emphasises the need for robust backups. Staff and students are advised to create copies of their data when saving files on work-supplied computers or on One Drive folders.

24. **Protection of Physical Infrastructure**

24.1 Servers are securely stored within lockable enclosures inside buildings, with data saved on secured Amazon Web Servers, compliant with GDPR.

SECTION 3

Responsibilities

25. Responsible usage of technological systems within IHM is entrusted to every department and individual.
26. Staff managing sensitive and confidential data have heightened responsibilities.
27. Staff members tasked with managing data related to students or colleagues bear heightened responsibility for cyber safety and security.
28. Inadequate protection of data could potentially expose individuals or IHM to legal violations, including breaches of the Federal Privacy Act (1988), the Victorian Information Privacy Act (2000), and other relevant legislation.

SECTION 4

Associated Information

Related Internal Documents	Bullying and Harassment Policy Bullying and Harassment Procedure Cyber Safety and Security Procedure Marketing of Courses to Overseas and Offshore Students Policy Marketing of Courses to Overseas and Offshore Students Procedure Privacy Policy Privacy Procedure Social Media Policy Social Media Procedure
Related Legislation, Standards, and Codes	Victoria's Cyber Strategy | vic.gov.au (www.vic.gov.au) Information Security Manual (ISM) | Cyber.gov.au Victorian Information Privacy Act (2000) Federal Privacy Act (1988),
Date Approved	02.08.2024
Date of Effect	03.08.2024
Date of Next Review	30.07.2027
Approval Authority	Audit and Risk Committee Endorsed by Board of Directors
Responsibility for implementation	Digital Transformation Department
Document Custodian	Head, Digital Transformation Department
IHM Doc ID	IHM-CSSP-2.0

Change History

Version Control		
Change Summary	Date	Short description of change, incl version number, changes, who considered, approved etc.
Version 1.1	22/02/2013	Ratification by Board of Governors
Version 1.2	23/11/2013	Version 1.2 approved by Board of Governors
Version 2.0	2/08/2024	• Policy and Procedure are separated into two documents • The definitions relocated to the glossary of terms • Template updated • Major update on incident response plan, regular training and awareness programs, periodic audits and assessments, data encryption, access controls and user permissions, multi-layered security approach, backup and recovery procedures, monitoring and reporting mechanisms, compliance with updated Regulations